FIG. 1

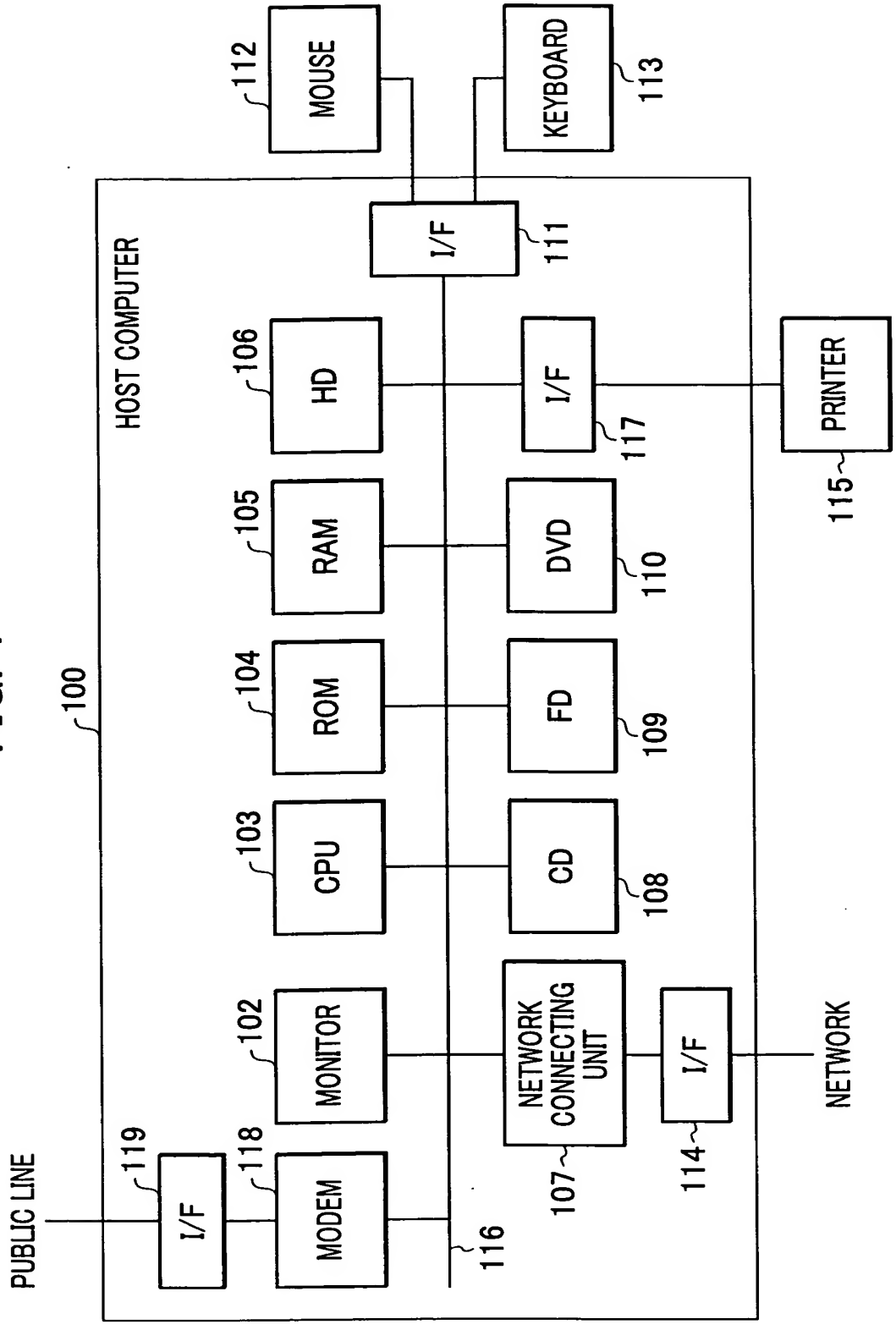

HOST COMPUTER
100
MOUSE
112
KEYBOARD
113
I/F
111
HD
106
I/F
117
PRINTER
115
RAM
105
DVD
110
ROM
104
FD
109
CPU
103
CD
108
MONITOR
102
NETWORK CONNECTING UNIT
I/F
114
NETWORK
PUBLIC LINE
I/F
119
MODEM
118
116
107

FIG. 2

	PROCESS 2-1	PROCESS 2-2
1		x
1	$(x)^2=x^2$	$x^2 \cdot x=x^3$
0	$(x^3)^2=x^6$	x^6
1	$(x^6)^2=x^{12}$	$x^{12} \cdot x=x^{13}$
1	$(x^{13})^2=x^{26}$	$x^{26} \cdot x=x^{27}$
1	$(x^{27})^2=x^{54}$	$x^{54} \cdot x=x^{55}$

FIG. 3

	PROCESS 2-1	PROCESS 2-2
11		x^3
01	$(x^3)^4=x^{12}$	$x^{12} \cdot x=x^{13}$
11	$(x^{13})^4=x^{52}$	$x^{52} \cdot x^3=x^{55}$

FIG. 4

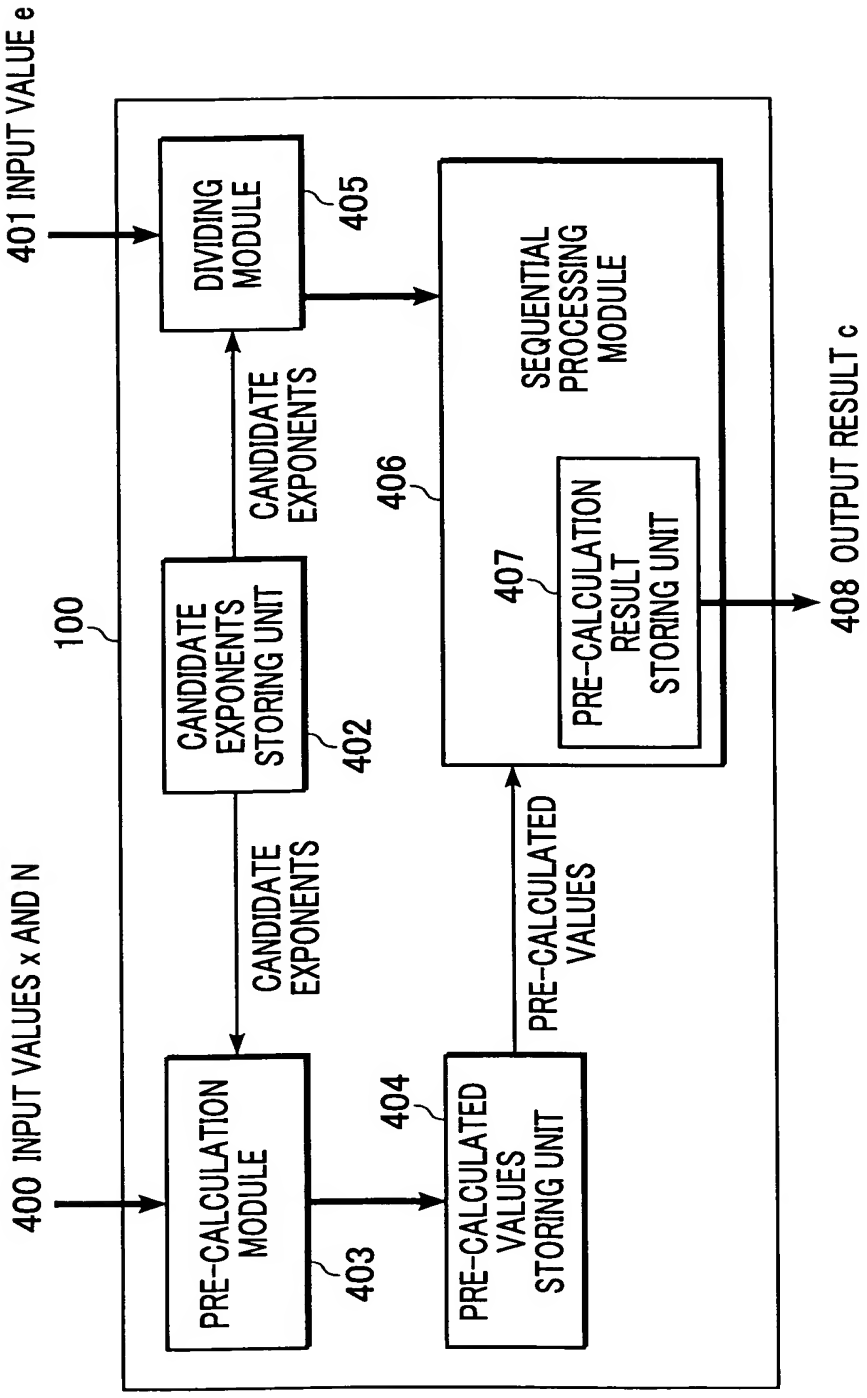

400 INPUT VALUES x AND N
401 INPUT VALUE e
100
PRE-CALCULATION MODULE
403
CANDIDATE EXPONENTS
CANDIDATE EXPONENTS STORING UNIT
402
DIVIDING MODULE
405
PRE-CALCULATED VALUES STORING UNIT
404
PRE-CALCULATED VALUES
SEQUENTIAL PROCESSING MODULE
406
PRE-CALCULATION RESULT STORING UNIT
407
408 OUTPUT RESULT c

FIG. 5

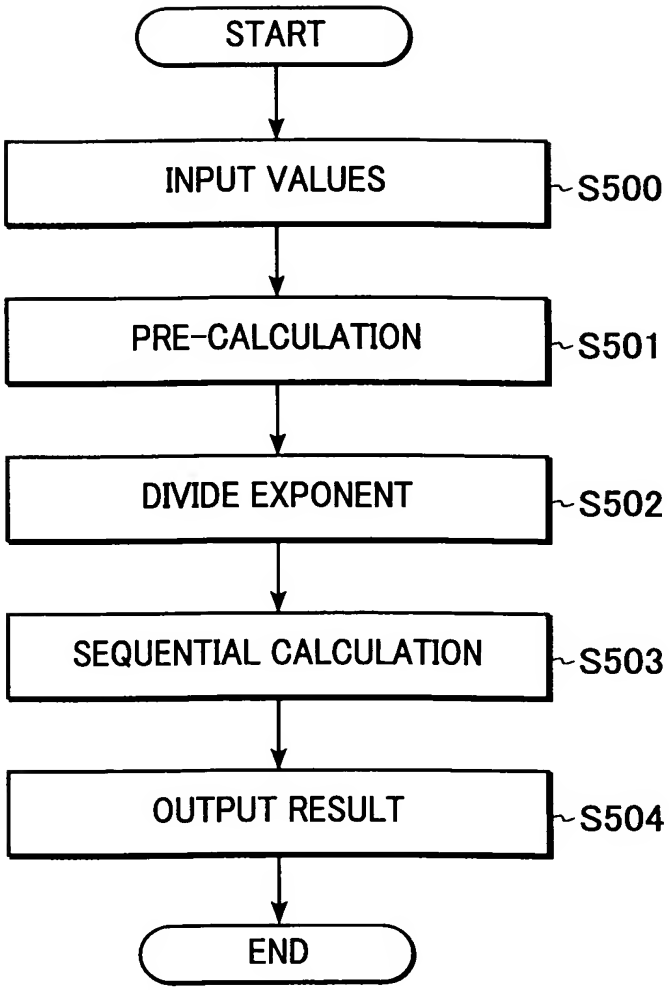

START
INPUT VALUES
S500
PRE-CALCULATION
S501
DIVIDE EXPONENT
S502
SEQUENTIAL CALCULATION
S503
OUTPUT RESULT
S504
END

FIG. 6

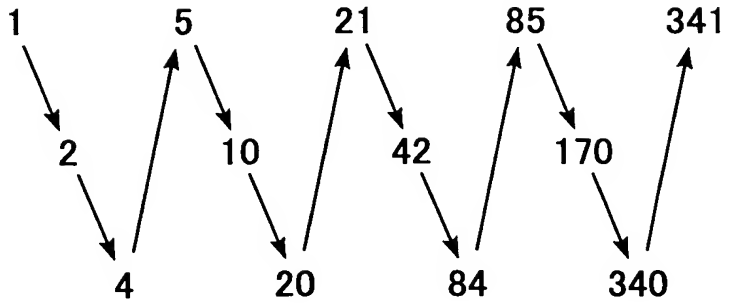


FIG. 7

e= 1101101110001010001

1 101 101 1 1 0 0 0 101 0 0 0 1

f_0 f_1···

FIG. 8

	STEP S503 PROCESS 1	PROCESS 2
1		x^1
101	$(x^1)^8 = x^8$	$x^8 \cdot x^5 = x^{13}$
101	$(x^{13})^8 = x^{104}$	$x^{104} \cdot x^5 = x^{109}$
1	$(x^{109})^2 = x^{218}$	$x^{218} \cdot x^1 = x^{219}$
1	$(x^{219})^2 = x^{438}$	$x^{438} \cdot x^1 = x^{439}$
0	$(x^{439})^2 = x^{878}$	$= x^{878}$

FIG. 9

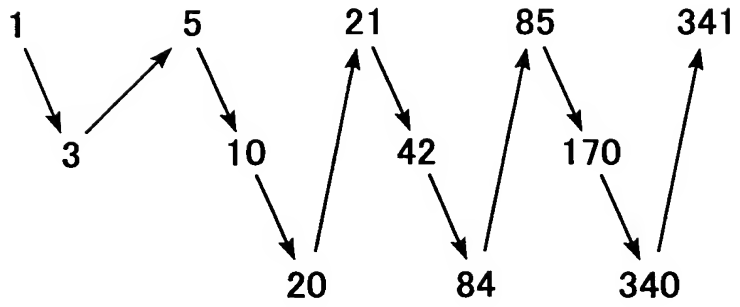


FIG. 10

e=11011011100010100 01

1 101 101 11 0 0 0 101 0 0 0 1

FIG. 11

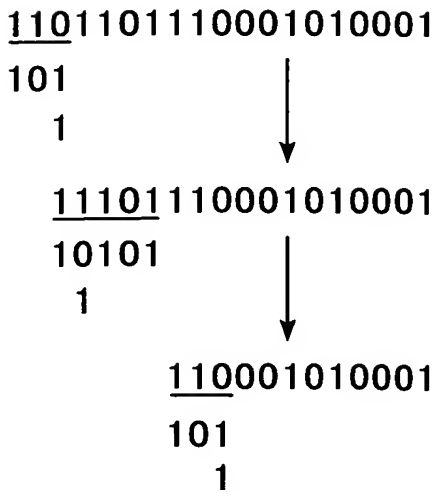


FIG. 12

		f_i, b_i	f_(i+1), b_(i+1)	sht
100		1, 1	–	2
101		101, 3	–	0
110	0	11, 2	–	2
	1	1, 1	101, 3	0
111	0	101, 1	1, 1	2
	1	101, 1	101, 3	0

FIG. 13

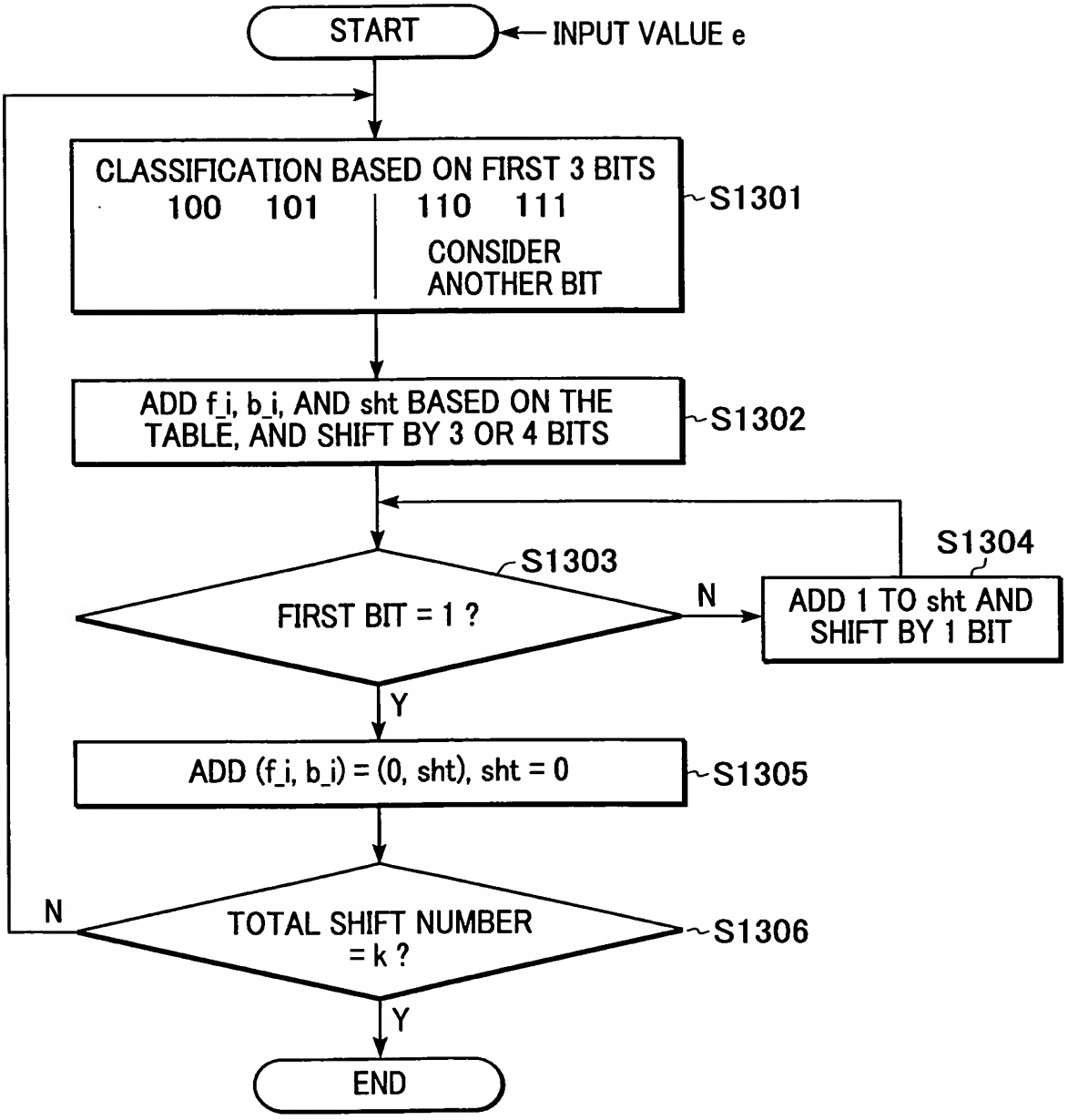

START
INPUT VALUE e
CLASSIFICATION BASED ON FIRST 3 BITS
100 101
110 111
CONSIDER ANOTHER BIT
S1301
ADD f_i, b_i, AND sht BASED ON THE TABLE, AND SHIFT BY 3 OR 4 BITS
S1302
S1303
FIRST BIT = 1 ?
N
S1304
ADD 1 TO sht AND SHIFT BY 1 BIT
Y
ADD (f_i, b_i) = (0, sht), sht = 0
S1305
N
TOTAL SHIFT NUMBER = k ?
S1306
Y
END

FIG. 14

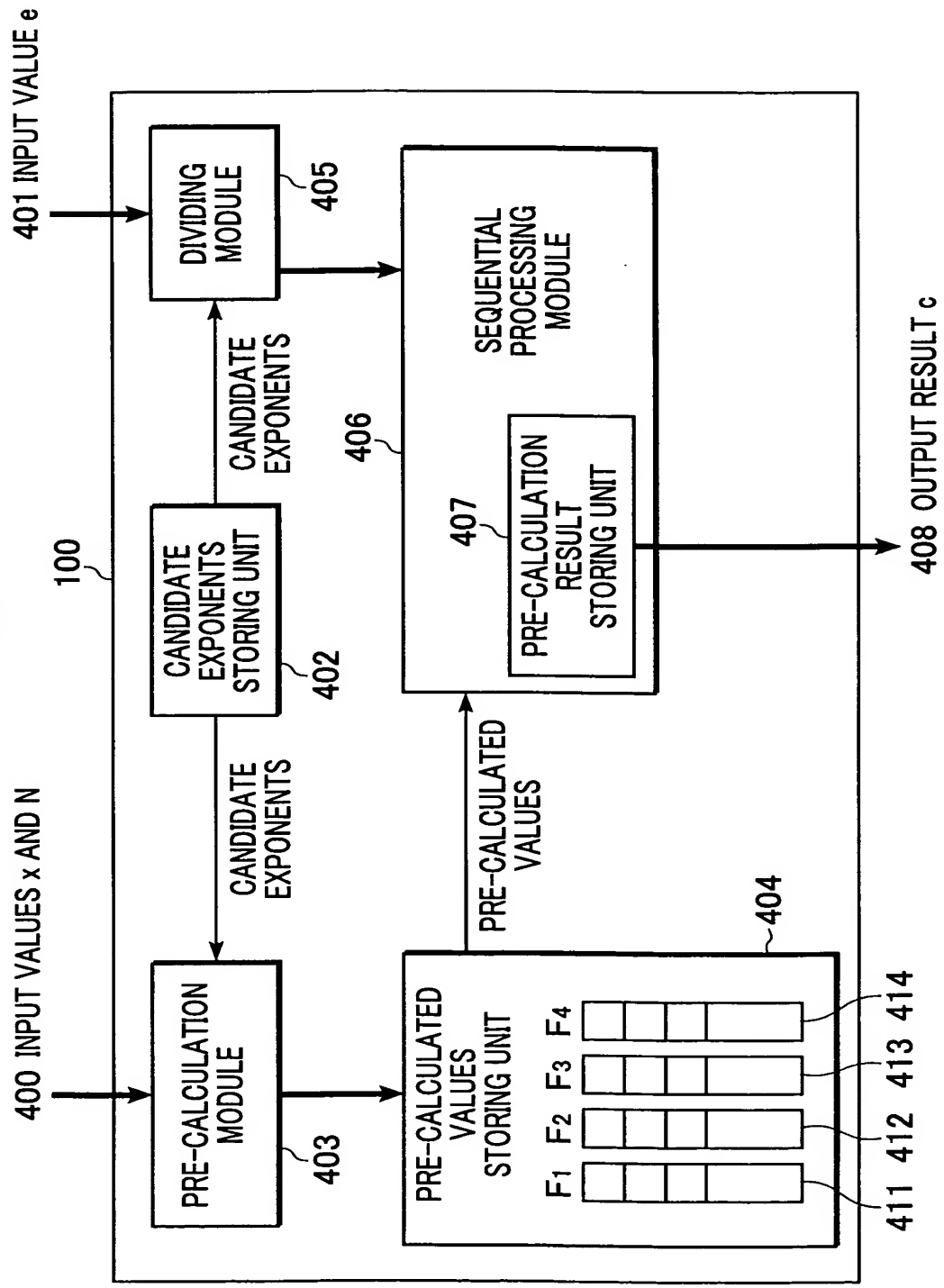

400 INPUT VALUES x AND N
401 INPUT VALUE e
100
PRE-CALCULATION MODULE
403
DIVIDING MODULE
405
CANDIDATE EXPONENTS STORING UNIT
402
CANDIDATE EXPONENTS
CANDIDATE EXPONENTS
PRE-CALCULATED VALUES
PRE-CALCULATED VALUES STORING UNIT
404
F1 F2 F3 F4
411 412 413 414
SEQUENTIAL PROCESSING MODULE
406
PRE-CALCULATION RESULT STORING UNIT
407
408 OUTPUT RESULT c

FIG. 15

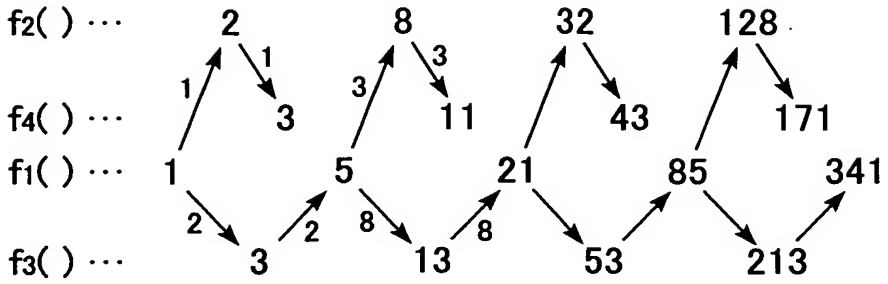


FIG. 16

e= 1101101111001010001

1101 1011 11 0 0 101 0 0 0 1

f_0 f_1···

FIG. 17

	STEP S503 PROCESS 1	PROCESS 2
1101		x^{13}
1011	$(x^{13})^{16} = x^{208}$	$x^{208} \cdot x^{11} = x^{219}$
11	$(x^{219})^{4} = x^{876}$	$x^{876} \cdot x^{3} = x^{879}$
0	$(x^{879})^{2} = x^{1758}$	$= x^{1758}$
0	$(x^{1758})^{2} = x^{3516}$	$= x^{3516}$
101	$(x^{3516})^{8} = x^{28128}$	$x^{28128} \cdot x^{5} = x^{28133}$
...	...	...

FIG. 18

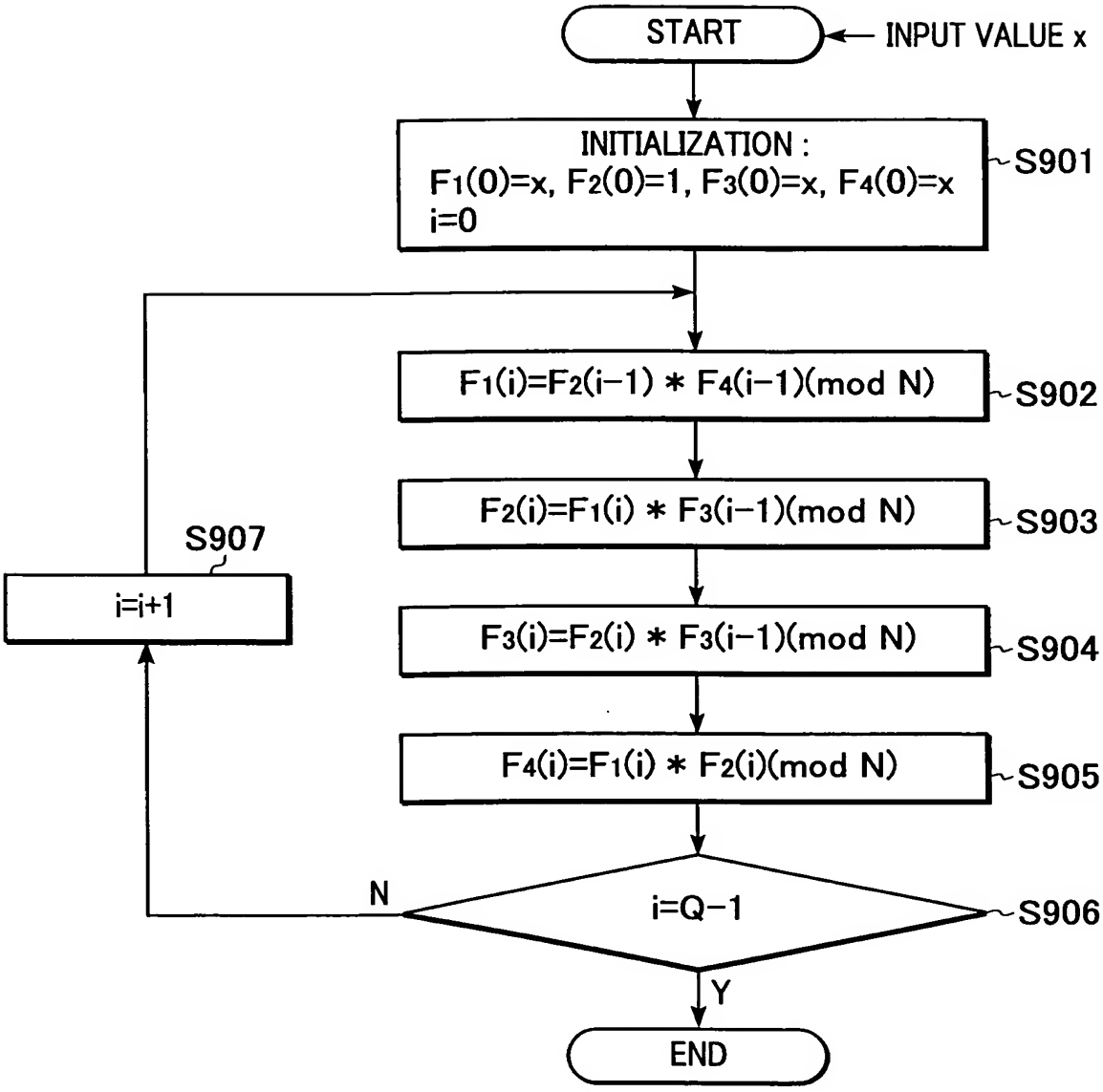
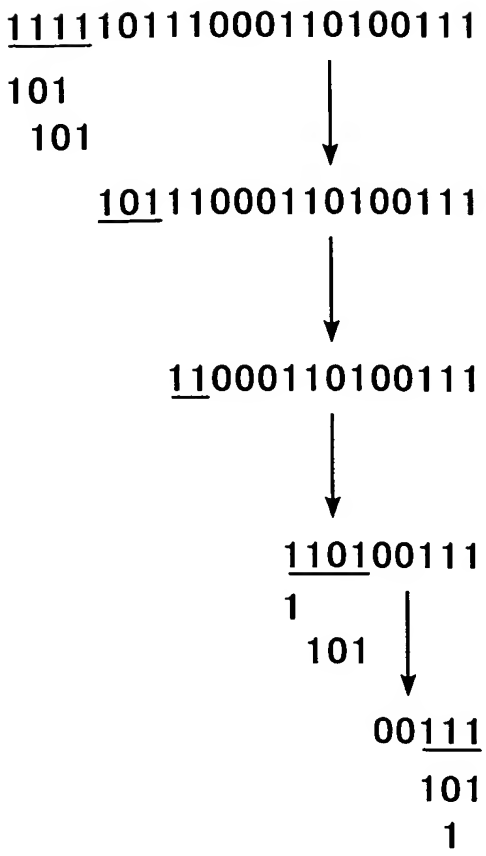

START
INPUT VALUE x
INITIALIZATION :
F1(0)=x, F2(0)=1, F3(0)=x, F4(0)=x
i=0
S901
F1(i)=F2(i−1) * F4(i−1)(mod N)
S902
F2(i)=F1(i) * F3(i−1)(mod N)
S903
F3(i)=F2(i) * F3(i−1)(mod N)
S904
F4(i)=F1(i) * F2(i)(mod N)
S905
i=Q−1
S906
N
Y
S907
i=i+1
END

FIG. 19


1111101111000110100111
101
101
101111000110100111
11000110100111
110100111
1
101
00111
101
1